

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of managing a communication with a mobile device over a network, comprising:

receiving a request from the mobile device, wherein the request includes associated information;

automatically determining at least one level of trust from a plurality of different levels of trust based, in part, on the associated information; and

determining at least one device signature for the mobile device based on the at least one level of trust from the plurality of different levels of trust, and independent of user authentication.

2. (Original) The method of Claim 1, further comprising:

receiving gateway information, wherein the gateway information is associated with a carrier gateway for the mobile device; and

determining the at least one level of trust based, in part, on the associated information and the gateway information.

3. (Original) The method of Claim 1, wherein the associated information comprises at least one of a device identifier, user agent information, and an indication that the mobile device is enabled to accept a cookie.

4. (Original) The method of Claim 3, wherein the associated information further comprises at least one of a gateway group identifier, and a subscription identifier.

5. (Currently Amended) The method of Claim 1, wherein the method further comprises:
automatically determining ~~another~~ a second level of trust from the plurality of different levels of trust based, in part, on the associated information; and

determining a second device signature for the mobile device based on the ~~other~~ second level of trust, and independent of user authentication.

6. (Original) The method of Claim 1, wherein the associated information further comprises a subscription identifier associated with the mobile device that is based on at least one of a Mobile Identification Number, an Electronic Serial Number, and an application serial number.

7. (Original) The method of Claim 1, wherein determining the at least one level of trust further comprises:

if the associated information comprises a device identifier and trustworthy gateway information, determining a first level of trust.

8. (Original) The method of Claim 1, wherein determining the at least one level of trust further comprises:

if the associated information indicates the mobile device is enabled to accept a cookie, determining a second level of trust.

9. (Original) The method of Claim 1, wherein determining the at least one level of trust further comprises:

if the associated information indicates the mobile device is enabled to use a URL, determining a third level of trust.

10. (Original) The method of Claim 1, wherein determining at least one device signature further comprises:

if a first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, a user agent identifier, and a time stamp.

11. (Original) The method of Claim 1, wherein determining at least one device signature further comprises:

if a second level of trust is determined, determining a second tier device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, a user agent identifier, and a time stamp.

receiving at least one device signature associated with the mobile device, wherein the at least one device signature is based on at least one level of trust determined from a plurality of different trust levels, and is independent of user authentication.

19. (Original) The client of Claim 18, wherein the client is configured to perform actions, further comprising:

providing a device identifier based on at least one of a Mobile Identification Number, an Electronic Serial Number, and an application serial number.

20. (Original) The client of Claim 18, wherein receiving the at least one device signature further comprises:

if the at least one device signature is based on a first level of trust, receiving a first tier device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, the user agent identifier, and a time stamp.

21. (Original) The client of Claim 18, wherein receiving the at least one device signature further comprises:

if the at least one device signature is based on a second level of trust, receiving a second tier device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, the user agent identifier, and a time stamp.

22. (Original) The client of Claim 18, wherein receiving the at least one device signature further comprises:

if the at least one device signature is based on a third level of trust, receiving a third tier device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp.

23. (Original) The client of Claim 18, wherein sending the request further comprises sending the request to a carrier gateway, wherein the carrier gateway is configured to perform actions, comprising:

modifying the request to include at least one of a subscription identifier associated with the mobile device, and a gateway identifier;

forwarding the modified request to the server;

receiving the at least one device signature from the server; and

forwarding the at least one device signature to the mobile device.

24. (Original) The client of Claim 18, wherein receiving the at least one device signature further comprises, if the request indicates the mobile device is enabled to accept a cookie, associating the cookie with the at least one device signature.

25. (Original) The client of Claim 18, wherein receiving the at least one device signature further comprises, associating a munged Uniform Resource Locator (URL) with the at least one device signature.

26. (Currently Amended) A server for managing a communication with a mobile device over a network, comprising:

a transceiver for receiving a request from the mobile device and for sending at least one device signature to the mobile device; and

a transcoder that is configured to perform actions, including:

receiving the request from the mobile device, wherein the request includes associated information;

automatically determining at least one level of trust from a plurality of different trust levels based, in part, on the associated information; and

determining the at least one device signature for the mobile device based on the at least one level of trust of the plurality of different trust levels, wherein the at least one device signature is independent of user authentication.

27. (Original) The server of Claim 26, wherein the transcoder is configured to perform further action, comprising:

receiving gateway information, wherein the gateway information is associated with a carrier gateway for the mobile device; and

32. (Original) The server of Claim 26, wherein determining the at least one level of trust further comprises determining a second level of trust based at least one of a gateway identifier, a user agent, and whether the mobile device is enabled to accept a cookie,.

33. (Original) The server of claim 26, wherein determining the at least one level of trust further comprises determining a third level of trust if the mobile device is enabled to interact with a URL.

34. (Original) The server of claim 26, wherein the transcoder is configured to perform further actions, comprising:

determining if at least one device signature has expired device, and

if the expired device signature is to be rolled over, extending a validity period associated with the expired device signature.

35. (Currently Amended) A system for managing a communication with a mobile device over a network comprising:

the mobile device configured to provide information associated with the mobile device;

and

a server, coupled to the carrier gateway, that is configured to receive the associated information and to perform actions, including:

automatically determining at least two different levels ~~one level~~ of trust from a plurality of different levels of trust based, in part, on the associated information; and

initially determining at least two different device signatures for the mobile device each of the two devices signatures being based on a different one of the at least two different levels ~~the at least one level~~ of trust, wherein the at least two device signatures are each determined independent of user authentication.

36. (Previously Presented) The system of Claim 35, wherein determining the at least two device signatures further comprises determining a tier 1 device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, a user agent identifier, and a time stamp.

37. (Previously Presented) The system of Claim 35, wherein determining the at least two device signatures further comprises determining a tier 2 device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, a user agent identifier, and a time stamp.

